UNITED STATES DISTRICT COURT

for the

Southern District of West Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information Associated with ted_kern3@msn.com that is Stored at Premises Controlled by Microsoft Corporation

Case No. 5:20-mj-00019

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment "A"

located in the Southern District of West Virginia, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 1341, 1343, 1349, 1956, 1957	Mail fraud, wire fraud, money laundering, and conspiracy to commit those offenses

The application is based on these facts:

See Attached Affidavit

- ☑ Continued on the attached sheet.
- ☑ Delayed notice of 30 days *(give exact ending date if more than 30 days: _____)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Michael Moyer, Special Agent FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by _____ *(specify reliable electronic means)*.

Date: April 10, 2020

City and state: Charleston, West Virginia

Omar J. Aboulhosn
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with ted_kern3@msn.com that is stored at premises owned, maintained, controlled, or operated by Microsoft, a company headquartered at One Microsoft Way, Redmond, WA 98052-6399.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Microsoft (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account between **May 1, 2012 and March 26, 2020**, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register

the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

f. The Provider is hereby ordered to disclose the above information to the government within **14 DAYS** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. §§ 1343 (wire fraud) and 1956-57 (money laundering), those violations involving **LEONARD THEODORE KERN** and occurring between **May 1, 2012 and March 26, 2020**, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Preparatory steps taken in furtherance of the scheme.

(b) Communications between KERN and B.M. (brendlou@yahoo.com).

(c) Communications between KERN and Hiram Ryan or Ryan Aerospace (hiram@ryanaerospace.com, *@ryanaerospace.com).

(d) Steps taken before and after inducement of B.M. to transfer money to KERN in 2012-2013.

(e) Steps taken before and after sending lulling communications to B.M. in furtherance of the scheme.

(f) Steps taken before and after receiving communications from Hiram Ryan.

(g) Steps taken after KERN was notified that he was served with a subpoena in May 2017 and September 2019.

(h) Communications between KERN and third-parties concerning financial transactions involving B.M.'s money.

(i) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(j) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(k) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(l) The identity of the person(s) who communicated with the user ID about matters relating to violations of 18 U.S.C. §§ 1343 (Wire Fraud), including records that help reveal their whereabouts.

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

STATE OF WEST VIRGINIA
COUNTY OF KANAWHA, to-wit:

I, Michael Moyer, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled by Microsoft Corporation, an email provider headquartered at One Microsoft Way, Redmond, WA 98052-6399. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Microsoft Corporation to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), assigned to the Huntington, West Virginia, Resident Agency Office of the Pittsburgh Division. I have been employed as a Special Agent for the FBI since January 2016. I am

currently tasked with investigating violations of federal law within the Southern District of West Virginia and elsewhere. As part of my duties, I have received training regarding the investigation of various federal crimes including, but not limited to, child exploitation, complex financial crimes, civil rights and violent crimes. By virtue of my FBI employment, I perform and have performed a variety of investigative tasks, including conducting arrests and the execution of federal search warrants and seizures. As a Special Agent, I am an investigative or law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7).

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1343 (Wire Fraud) and 1956-67 (money laundering) have been committed by LEONARD THEODORE KERN ("KERN"). There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. §§ 2711 and 2703. Specifically, the Court is "a district

court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND: INVESTMENT FRAUD SCHEMES

6. The F.B.I. has participated in numerous investigations of fraud activity commonly referred to as Platform Trading, Private Platform Programs (PPPs), Prime Bank Trading, or Medium-Term Note Trading Programs. In these schemes, perpetrators falsely represent their ability to offer above-average market returns with below-market risk through the trading of bank instruments.

7. The FBI has participated in numerous investigations of persons promoting Platform Trading investment schemes. Several common characteristics include claims that: (1) investor funds can be placed in a bank account and then used, without risk, to trade bank debentures or other financial instruments; (2) invested funds can be used to lease or rent U.S. Treasury Obligations and then use these same leased securities as collateral for further trading programs; (3) trading Medium Term Notes (MTNs), Prime Bank Notes, or any other bank instruments, on a riskless basis, will yield above market returns; (4) Letters of Credit or Standby Letters of Credit can be discounted or traded for profits; (5) certain high-yield foreign trading programs are sanctioned or supported by the Federal Reserve, International Monetary Fund, International Chamber of Commerce, or other U.S. or international agencies; (6) special connections to the Federal Reserve or some other internationally

renowned organization such as the United Nations, the IMF or the World Bank; (7) benevolent, humanitarian, or charitable projects; (8) the need for extreme secrecy and nondisclosure agreements; (9) banking and regulatory officials will deny knowledge of such instruments; (10) these investment opportunities are by invitation only, available to only a handful of special customers, and historically reserved for the wealthy elite; (11) the financial instruments are too technical or complex for non-experts to understand.

8. In general, investment programs that purport to offer an introduction to secret investment markets, which offer above-market rates of return with below-market rates of risk for privileged customers with special access, are fraudulent. There are no secret markets in Europe or in North America in which banks trade securities.

FACTUAL BACKGROUND

The facts in this section are derived from witness interviews with B.M. and other individuals, as well as documents and communications received from B.M., and financial and other documents reviewed during the course of my investigation:

9. B.M. inherited a scrap metal business in 2009 after B.M.'s father passed away. The business was started by B.M.'s grandfather and was located in Mabscott, Raleigh County, West Virginia, and

within the Southern District of West Virginia. B.M. worked for the family business most of her adult life.

10. In or about 2012, B.M. was contacted by a consulting firm who offered assistance to improve B.M.'s business. The company informed B.M. that KERN would be the consultant assigned to assist B.M.'s business. KERN travelled to West Virginia to provide consulting services. KERN provided business consulting services to B.M. from approximately January 2012 to May 2012.

11. KERN formed a professional relationship of trust with B.M., whereby KERN advised B.M. on the operations and finances of the business. KERN was paid approximately $13,000 per week which included per diem, hotel, airfare, automobile expenses and professional time for the consulting services.

12. During the time KERN was providing business consulting services to B.M. in West Virginia, KERN also formed a personal friendship with B.M., and B.M. shared personal information with KERN, including information regarding her personal finances.

13. B.M.'s business relationship with KERN ended after several months when B.M. informed KERN that B.M. was no longer able to afford the consulting services. KERN left West Virginia and returned to his home state of Texas.

14. In or about May 2012, KERN approached B.M. with a proposed "platform" investment in which B.M. would receive $1,000,000 in sixty days if B.M. would transfer $200,000 to KERN. B.M. sent a cashier's

check for $200,000 by mail to KERN, who deposited the check into a bank account that KERN created at Comerica Bank in Dallas, Texas. KERN instructed B.M. to keep the investment secret from everyone, including from her husband, and B.M. followed KERN's instruction.

15. In or about July 2012, KERN approached B.M. again and requested an additional $175,000 from B.M. KERN represented that the additional funds were needed in order to close a deal KERN was presently completing. KERN promised B.M. would receive $2,000,000 in sixty days. B.M. sent and additional $175,000 by wire transfer to KERN into a bank account that KERN created at Comerica Bank in Dallas, Texas.

16. On at least 80 occasions, from at least in or about July 2012 through in or about November 2019, KERN sent B.M. interstate wire communications, that is, electronic mail and text messages, on or about a weekly basis with excuses as to why B.M. had not received the promised return on B.M.'s money.

17. B.M never received the promised return on the money transferred to KERN, and B.M. suffered a loss of more than $375,000. KERN never revealed he used more than $100,000 of B.M.'s money for his personal benefit.

BACKGROUND OF THE INVESTIGATION

18. As part of my investigation, I have reviewed bank statements from Comerica Bank account (#XXX9922) for a company

created by KERN, Primo Classe Investment Corporation ("Primo"). The statements for the Primo account show the following transactions:

a. May 28, 2012: $200,000 check from B.M. to KERN deposited into the Primo account.

b. KERN immediately used the money received from B.M. for personal expenses by frequently using a debit card associated with the Primo account and withdrawing cash.

c. June 30, 2012: KERN wrote a check from the Primo account for $20,000 payable to David McDavid Lincoln Mercury to purchase a 2010 Lincoln Navigator.

d. July 2, 2012: Primo wire transferred $25,000 to Ryan Aerospace, a company created by an individual believed to be KERN's co-conspirator, Hiram Ryan.

e. July 9, 2012: B.M. sent a wire transfer to KERN for $175,000, which was deposited into Primo account.

f. July 10, 2012: Primo wire transferred $300,000 to Ryan Aerospace.

g. October 9, 2012: Ryan Aerospace wire transferred $20,000 to Primo.

h. November 14, 2012: Ryan Aerospace wire transferred $10,000 to Primo.

i. November 27, 2012: Ryan Aerospace wire transferred $5,000 to Primo.

j. December 5, 2012: Ryan Aerospace wire transferred $10,000 to Primo.

k. KERN used the money received from B.M. to make at least four monthly mortgage payments to Chase Bank in the amounts of $1,875.60 per month from July to December 2012.

l. B.M.'s funds were depleted to $849.30 by January 1, 2013.

m. January 15, 2013: B.M. sent a wire transfer to Primo for $3,000, which was deposited into the Primo account.

n. January 31, 2013: B.M. sent a wire transfer to Primo for $1,000, which was deposited into the Primo account.

o. February 8, 2013: B.M. sent a wire transfer to Primo for $2,000 which was deposited into Primo account.

p. February 27, 2013: B.M. sent a wire transfer to Primo for $1,500 which was deposited into Primo account.

q. March 14, 2013: B.M. sent a wire transfer to Primo for $2,500 which was deposited into Primo account.

r. March 28, 2013: B.M. sent a wire transfer to Primo for $1,500 which was deposited into Primo account.

s. September 30, 2014: Ryan Aerospace wire transferred $1,000 to Primo.

t. October 1, 2014: Ryan Aerospace wire transferred $1,000 to Primo.

u. October 2, 2014: Ryan Aerospace wire transferred $1,000 to Primo.

v. October 10, 2014: Ryan Aerospace wire transferred $1,000 to Primo.

19. Based on these bank records, it appears that KERN set up the Primo Account for the purpose of receiving B.M.'s funds and then immediately used approximately $100,000 of the funds for his personal benefit. B.M. has told investigators that B.M. did not authorize KERN to take any type of commission or fee from the $375,000 transferred to him by B.M.

20. KERN represented to B.M. that the entire $375,000 was jointly being placed into a "platform" investment with $50,000 of KERN's own funds and funds contributed by Hiram Ryan. Based on the bank records and a November 2019 interview of Ryan, KERN's representation to B.M. is false. Additionally, evidence of the existence of this financial transaction have been subpoenaed from Primo Classe Investments and Ryan Aerospace. However, no evidence of the financial transactions described by KERN to B.M. have been produced pursuant to the subpoenas.

21. In November 2019, Hiram Ryan told investigators that he was helping KERN arrange an investment deal with a third-party, Steve Allison. Ryan told investigators that he was merely passing on the money transferred to him by KERN to Allison. Ryan stated that he would have transferred the money to Allison within days of receiving it from KERN and would have likely only taken a nominal fee or commission for arranging the deal between KERN and Allison.

22. Bank statements for accounts held by Ryan Aerospace and Hiram Ryan have also been analyzed. As described above, KERN sent Ryan $275,000 of the funds KERN received from B.M. in May and July of 2012. No evidence of a subsequent wire transfer from Ryan to Allison was found in the bank records. The only notable wire transfer in the records was a transfer of $112,500 from Ryan to JR Capital LLC on December 7, 2012. The investigation into Ryan, Allison, and JR Capital LLC is ongoing. Investigators have not yet determined whether the December 7, 2012 transfer has any relation to the transaction involving KERN and B.M. However, even if the wire transfer of $112,500 was part of a legitimate investment transaction involving B.M.'s funds, it would mean that Hiram Ryan took a fee or commission of $162,500 out of the money transferred to him by KERN in addition to the $100,000 taken by KERN for his personal benefit.

23. Based on the extraordinarily high rate of return of the financial transaction proposed by KERN, KERN's deposit of the $375,000 in a new bank account set up to receive B.M.'s funds, KERN's use and concealment from B.M. of $100,000 of the funds for his personal benefit, Ryan's use of the funds received by KERN, the lack of evidence of the existence of any financial transaction described by KERN to B.M. produced in response to subpoenas, and my review of subsequent emails and text messages sent by KERN describing the nature of the investment, it appears that the $375,000 sent by B.M. to KERN in May and July of 2012 was taken by KERN as part of an

investment fraud scheme. The claims made by KERN when describing the nature of the investment to B.M. are generally consistent with Platform Trading investment fraud schemes. KERN proposed a "platform" investment to B.M. with an extremely high rate of return and drafted promissory notes to make the transaction appear less risky to B.M. KERN used complicated and technical terminology commonly used in investment fraud schemes to describe the investment to B.M., and KERN instructed to B.M. to keep the transfer a secret.

PROBABLE CAUSE TO SEARCH EMAIL ACCOUNT

24. I have reviewed copies of wire communications (emails) sent by KERN from his Microsoft email account, ted_kern3@msn.com, to B.M. These copies were received during the course of the investigation from B.M. and appear to have been sent by KERN between May 2012 and November 2019. Based on my review of the emails, it appears that KERN uses his Microsoft email account to communicate with B.M., as well as an individual believed to be KERN's co-conspirator, Hiram Ryan.

25. The emails KERN sent to B.M. from May 2012 until November 2019 contain excuses as to why B.M. had not received the promised return on B.M.'s money. The emails generally include descriptions of potential investment deals that KERN claimed he was personally in the process of completing. However, as discussed above, it appears that the $375,000 sent by B.M. to KERN in May and July of 2012 was taken by KERN as part of an investment fraud scheme and that KERN's

representations to B.M. about the status of her investment are false and designed to lull B.M. into a false sense of security, postpone inquiries and complaints, and make the financial transactions appear less suspect in furtherance of the scheme.

26. On or about May 19, 2012, KERN emailed B.M. a promissory note dated May 19, 2012, which showed Primo as the borrower and showed B.M. as the lender. The terms of the note showed the period of the loan was for sixty (60) days, with $800,000 in interest, and $200,000 in principal, for a total principal and interest payment of $1,000,000, payable to B.M. by July 23, 2012.

27. On or about July 2, 2012, KERN emailed B.M. a promissory note dated July 3, 2012, which modified the total loan amount to $375,000. The terms of the note showed the period of the loan was for sixty (60) days, with $1,625,000 in interest, and $375,000 in principal, for a total principal and interest payment of $2,000,000, payable to B.M. in two installments, on or around August 20, 2012 and by September 17, 2012.

28. On or about March 26, 2013, KERN emailed B.M. and represented that her $375,000 investment purchased a $5M standby letter of credit (SBLC). KERN provided a six-round breakdown of B.M.'s investment and attached a payout schedule in the form of a two-page spreadsheet to the email. KERN represented that B.M. would be paid $600,000 in "Round 1" which would be "this month." In "Round 2A," KERN represented B.M. would be paid another $600,000 "one month

after round 1." In "Round 3A," KERN represented that another investment would be made into a "$50M SBLC for IGR Foundation … one month after round 2A." In rounds 2B and 3B, KERN represented B.M. would be paid "$500K" one month after round 3A. In "Round 4B," KERN represented that "$20M" would be split "weekly for 40 weeks – starting 1 month after round 3B." KERN attached a two-page spreadsheet to the email purporting to be a detailed payout schedule beginning in October 2012 and ending in September 2013 wherein B.M. was shown to receive a grand total of $394,916,667 in payments from the investment over 59 weeks.

29. On or about April 8, 2013, KERN emailed B.M. stating, "We had a choice of two Traders who were willing to start with a smaller amount at $375K rather than the usual $1.2M. We were with a [Venezuelan] Central Bank Trader up through December. The political unrest in that country made us very nervous. Now that their President/Dictator, Hugo Chavez is dead, the [Venezuela] Trades have all stopped. What they didn't tell us was that we would be re-prioritized based upon our investment amount at each stage of this initial transaction. We are now at the final step and are all feeling frustrated about continuing to be re-prioritized around by bigger deals. I did check a week ago about what we could get back if we called it quits and the answer came back that since we've already bought the SBLC and we've already gotten a loan against it, the fees charged to quit now would eat up all but about $50K - $75K. Going

forward is really the best option. There is no upside to [quitting] at this point. Our Trader's problem is that his bank's smallest SBLC is $20M, not the $5M that we have. He went to a different bank for the SBLC for us and he doesn't have the same amount of control to prioritize and push things through like he would at his bank. Each of the next rounds is larger than $20M and will be at his bank, we just need this first domino to go ahead and fall over. Before we got involved with this guy, we saw bank statements from two other groups who had worked with him. He is legitimate. Nobody has run away with anything and they are still taking our calls. This is frustrating, but we are so close and the upside is so high, that it would be foolish to stop now. Regards, Ted."

30. On or about October 24, 2013, KERN emailed B.M. and represented that, "[B.M.], I am so sorry that I have been out of touch the last few days… I haven't called into today's call yet, but my prediction is that we should have movement next week, based on what I have heard. It is insane that we are coming up to an anniversary date with this particular group. Hiram has a third group of investors that if they sign up, will pay us enough fees to get you [and] your original investment back. I would prefer for the deal to go through because that would get you alot [sic] more and set you up for life. I almost hate telling you about this group since they haven't signed the papers yet but Hiram and I both feel very guilty for this deal to be taking as long as it has. I will call you tomorrow

on the way home to give you a full run down on our deal and any progress that Hiram may be having on the alternative. Ted."

31. On or about October 1, 2014, KERN emailed B.M. and represented that, "[B.M.], I am doing well. Thank you for asking. Normally, I would have called you with this update, but since you seem to want to take things to a more formal level, based on the tone of your note yesterday, I am giving you this week's update in writing. As I have said in the past and also confirmed by Hiram on the letter to you on 9/12/14, we both are committed to a full payment of your principal and interest due to you under the Promissory Note you received from Primo Classe Investment Corp on 7/3/12. I am also committed to repaying you $11,500 you loaned me personally as well. The primary issue with the transaction you are involved in is the small size of it when compared to other transactions in this arena. Hiram and I are both close to closing other investment transactions that are significantly larger in size and able to go through the system at the speed we originally expected yours to have. If any of these deals close before our $5M SBLC deal monetizes at the bank, we will use any of the proceeds due us to repay you. I have re-confirmed yesterday that a European investor for me is planning on wiring funds from his Swiss account on Monday, 10/6/14. Within one week of his wiring, Primo Classe Investment Corp will be able to wire your first scheduled payment of $600,000 and I will be able to wire you the $11,500 I owe you as well. Your second payment of $600,000 would be

3-4 weeks after that. Hiram and I are still chasing the $5M SBLC on the original deal and hope to have movement soon on that project. Whichever project hits first, we will get you paid. I have attached a copy of the authorization form for funds transfer from our transaction: 1. Purchase the next 20M euro SBLC for $1,125,000. 2. Retain the investment of $450,000 on the original $5M SBLC. 3. Return an excess of $1,803,500 to Ryan Aerospace, to be split three ways between [B.M.], Hiram, and Ted. I am somewhat surprised to see that you feel I don't worry about what happens to you. Hiram can attest that on nearly every conversation we have, I am always thinking about how we can take care of [B.M.]. Regards, Ted Kern President Primo Classe Investment Corp." KERN attached what was purported to be a copy of an "authorization for funds transfer" relating to the transaction with B.M.

32. On or about March 24, 2015, KERN emailed B.M., and represented that, "[B.M.], We are still waiting for the funds to clear and had to create a cover letter to organize the attachments presented to the bank so that everything weaves together and passes their compliance audit. My best guess right now is that we moved from a 4/3 clearing date to some time in the following week. Ted." KERN attached documents to the email purporting to show the existence of a financial transaction between KERN and third parties concerning a five-billion Euro bank draft issued to a "Philippine humanitarian

philanthropist citizen" by the name of "Milagros Rodriguez Tumimbang."

33. On or about November 3, 2016, KERN emailed B.M., and represented that, "[B.M.], Hot off the presses. After every delay excuse we've gotten, the first transfer is to go out tomorrow morning with 4 more scheduled every other Friday. Tomorrow, I can get a confirmation and let you know. Ted."

34. The emails referenced above are consistent with a lulling fraud scheme. In each email, KERN represents that a return on B.M.'s money is likely to happen within days. The emails are designed by KERN to convince B.M. that B.M.'s funds are being properly managed and to lull B.M.'s concerns about the legitimacy of the financial transaction.

35. There is probable cause to believe that there are additional emails from/to KERN to/from B.M. and Hiram Ryan stored in KERN's "mail box" on Microsoft servers. There is probable cause to believe that additional emails stored in KERN's mail box relating to the existence of the purported deals KERN described to B.M. during the course of the scheme. In general, an email that is sent to a Microsoft subscriber is stored in the subscriber's "mail box" on Microsoft servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Microsoft servers indefinitely. Even if the subscriber deletes the

email, it may continue to be available on Microsoft's servers for a certain period of time.

BACKGROUND CONCERNING EMAIL

36. In my training and experience, I have learned that Microsoft provides a variety of on-line services, including electronic mail ("email") access, to the public. Microsoft allows subscribers to obtain email accounts at the domain name msn.com, like the email account[s] listed in Attachment A. Subscribers obtain an account by registering with Microsoft. During the registration process, Microsoft asks subscribers to provide basic personal information. Therefore, the computers of Microsoft are likely to contain stored electronic communications (including retrieved and unretrieved email for Microsoft subscribers) and information concerning subscribers and their use of Microsoft services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

37. A Microsoft subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Microsoft. In my training and experience, evidence of who was using an email

account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

38. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

39. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and

other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

40. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

41. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in

connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or

consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

42. Based on the forgoing, I request that the Court issue the proposed search warrant.

43. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Microsoft. Because the warrant will be served on Microsoft, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Further your affiant sayeth naught.

SPECIAL AGENT MICHAEL MOYER,
FEDERAL BUREAU OF INVESTIGATION

Sworn to before me, and subscribed ~~in my presence~~, this 10th Day of April, 2020, pursuant to Rule 4.1 F.R.Cr.P.

Omar J. Aboulhosn
United States Magistrate Judge

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Microsoft, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Microsoft. The attached records consist of _____. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Microsoft, and they were made by Microsoft as a regular practice; and

b. such records were generated by Microsoft's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Microsoft in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Microsoft, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature